



Initiation aux réseaux

Concept de réseau

Un **réseau** est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

Selon le type d'objets, on parlera parfois de :

- **Réseau de transport** : ensemble d'infrastructures et de disposition permettant de transporter des personnes et des biens entre plusieurs zones géographiques.
- **Réseau téléphonique** : infrastructure permettant de faire circuler la voix entre plusieurs postes téléphoniques.
- **Réseau de neurones** : ensemble de cellules interconnectées entre elles.
- **Réseau de malfaiteurs** : ensemble d'escrocs qui sont en contact les uns avec les autres (un escroc en cache généralement un autre !)
- **Réseau informatique** : ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (des valeurs binaires, c'est-à-dire codées sous forme de signaux pouvant prendre deux valeurs : 0 et 1).

Le présent ouvrage s'intéressera bien évidemment aux réseaux informatiques.

Il n'existe pas un seul type de réseaux, car historiquement il existe des types d'ordinateurs différents, communiquant selon des

langages divers et variés. De plus, les supports physiques de transmission les reliant peuvent être très hétérogènes, que ce soit au niveau du transfert de données (circulation de données sous forme d'impulsions électriques, sous forme de lumière ou bien sous forme d'ondes électromagnétiques) ou bien au niveau du type de support (lignes en cuivres, en câble coaxial, en fibre optique...).

Les différents chapitres suivants s'attacheront à décrire les caractéristiques des supports physiques des transmissions, ainsi que la manière dont les données transitent sur le réseau.



À savoir

Réseau (*network*) : c'est l'ensemble des ordinateurs et périphériques connectés les uns aux autres. Deux ordinateurs connectés constituent déjà un réseau.

Mise en réseau (*networking*) : c'est la mise en œuvre des outils et des tâches permettant de relier des ordinateurs afin qu'ils puissent partager des ressources.

Intérêt d'un réseau

Un **ordinateur** est une machine permettant de manipuler des données. L'homme, en tant qu'être communicant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations.

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels).
- La communication entre personnes (courrier électronique, discussion en direct, etc.).
- La communication entre processus (entre des machines industrielles par exemple).
- La garantie de l'unicité de l'information (bases de données).
- Le jeu vidéo multijoueurs.

Les réseaux permettent aussi de standardiser les applications, on parle généralement de **groupware**. Par exemple, la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement.

Voici les avantages qu'offrent de tels systèmes :

- diminution des coûts grâce aux partages des données et des périphériques,
- standardisation des applications,
- accès aux données en temps utile,
- communication et organisation plus efficace.

Aujourd'hui, la tendance est au développement vers des **réseaux étendus** (WAN) déployés à l'échelle du pays, voire à l'échelle mondiale. Ainsi, les intérêts sont multiples, que ce soit pour une entreprise ou pour un particulier.

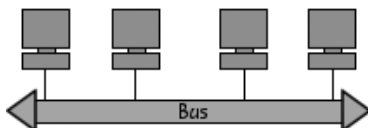
Topologie d'un réseau

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, liaisons sans fil, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé **topologie physique**. On distingue généralement les topologies suivantes :

- la topologie en bus,
- la topologie en étoile,
- la topologie en anneau,
- la topologie en arbre,
- la topologie maillée.

La **topologie logique**, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

Topologie en bus



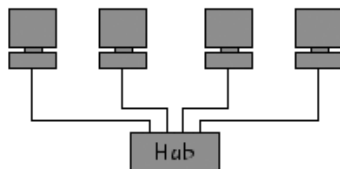
Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles, généralement de type coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

Topologie en étoile

Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un système matériel central appelé **concentrateur** (*hub*, littéralement *moyen de roue*). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Le concentrateur a pour rôle d'assurer la communication entre les différentes jonctions.

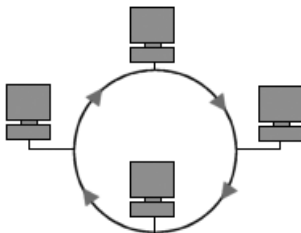
Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.



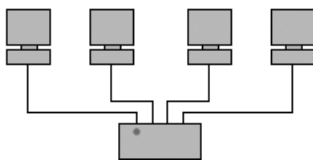
En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le concentrateur).

Topologie en anneau

Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.



En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (MAU, *Multistation Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant, à chacun d'entre eux, un « temps de parole ».



Les deux principales topologies logiques utilisant cette topologie physique sont Token Ring (anneau à jeton) et FDDI.

Architectures réseaux

En élargissant le contexte de la définition du réseau aux services qu'il apporte, il est possible de distinguer deux modes de fonctionnement :

- **l'architecture d'égal à égal** (*peer to peer*, parfois appelée « poste à poste »), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur joue un rôle similaire,
- **l'architecture de type client-serveur**, où un ordinateur (serveur) fournit des services réseau aux ordinateurs clients.

Architecture d'égal à égal

Dans une architecture d'**égal à égal** (ou *poste à poste*), contrairement à une architecture de réseau de type client-serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau est un peu serveur et un peu client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder *via* le réseau.

❑ Inconvénients

Les réseaux d'égal à égal ont énormément d'inconvénients :

- ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer,
- la sécurité est très peu présente,
- aucun maillon du système n'est fiable.

Ainsi, les réseaux d'égal à égal ne sont valables que pour un petit nombre d'ordinateurs (généralement une dizaine), et pour des applications ne nécessitant pas une grande sécurité (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

❑ Avantages

L'architecture d'égal à égal a tout de même quelques avantages parmi lesquels :

- **un coût réduit** (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance),
- **une simplicité** à toute épreuve !

❑ Mise en œuvre d'un réseau poste à poste

Les **réseaux poste à poste** ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour

serveurs dédiés. On peut donc utiliser les différentes versions de Windows car tous ces systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

La mise en œuvre d'une telle architecture réseau repose sur des solutions standards :

- placer les ordinateurs sur le bureau des utilisateurs,
- chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité,
- pour les connexions, on utilise un système de câblage simple et apparent.

Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :

- moins de 10 utilisateurs,
- tous les utilisateurs sont situés dans une même zone géographique,
- la sécurité n'est pas un problème crucial,
- ni l'entreprise ni le réseau ne sont susceptibles d'évoluer de manière significative dans un proche avenir.

Administration d'un réseau poste à poste

On désigne par le terme **administration** :

- la gestion des utilisateurs et de la sécurité,
- la mise à disposition des ressources,
- la maintenance des applications et des données,
- l'installation et la mise à niveau des logiciels utilisateurs.

Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. Tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, etc.).

Notions de sécurité

La politique de **sécurité minimale** consiste à mettre un mot de passe à une ressource. Les utilisateurs d'un réseau poste à poste définissent leur propre sécurité et, comme tous les partages peuvent exister sur tous les ordinateurs, il est difficile de mettre en œuvre un contrôle centralisé. Ceci pose également un problème de

sécurité globale du réseau car certains utilisateurs ne sécurisent pas du tout leurs ressources.

Architecture client/serveur

De nombreuses applications fonctionnent selon un environnement client-serveur, cela signifie que des **machines clientes** (des machines faisant partie du réseau) contactent un **serveur**, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des **services**. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion...

Les services sont exploités par des programmes, appelés **programmes clients**, s'exécutant sur les machines clientes. On parle ainsi de client FTP, client de messagerie... lorsque l'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client messagerie il s'agit de courrier électronique).

Dans un environnement purement client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est un des principaux atouts de ce modèle.

□ Avantages

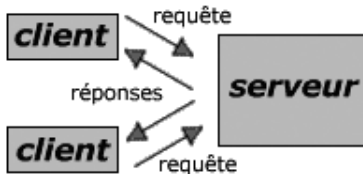
Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- **des ressources centralisées** : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction ;
- **une meilleure sécurité** : car le nombre de points d'entrée permettant l'accès aux données est moins important ;
- **une administration au niveau serveur** : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés ;
- **un réseau évolutif** : grâce à cette architecture il est possible de supprimer ou de rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures.

❑ Inconvénients

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- **un coût élevé** : dû à la technicité du serveur ;



- **un maillon faible** : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID).

❑ Fonctionnement d'un système client/serveur

Un système client/serveur fonctionne selon le schéma suivant :

- Le client émet une requête vers le serveur grâce à son adresse et le port qui désigne un service particulier du serveur.
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port.

Familles de réseaux

On distingue différents types de réseaux selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On définit généralement les catégories de réseaux suivantes :

- **Réseaux personnels** ou PAN (*Personal Area Network*).
- **Réseaux locaux** ou LAN (*Local Area Network*).
- **Réseaux métropolitains** ou MAN (*Metropolitan Area Network*).
- **Réseaux étendus** ou WAN (*Wide Area Network*).

Il existe d'autres types de réseaux tels que les **TAN** (*Tiny Area Network*) identiques aux LAN mais moins étendus (deux à trois machines) ou les **CAN** (*Campus Area Network*) identiques au MAN avec une bande passante maximale entre tous les LAN du réseau.

Réseaux locaux (LAN)

Un réseau local (**LAN**, *Local Area Network*) désigne un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet standard) à 1 Gbps (Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1 000 machines.

En élargissant le contexte de la définition aux services qu'apporte le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement **d'égal à égal** (*peer to peer*), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire ;
- dans un environnement **client/serveur**, dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

Réseaux métropolitains (MAN)

Les réseaux métropolitains (**MAN**, *Metropolitan Area Network*) interconnectent plusieurs réseaux locaux géographiquement proches (au maximum quelques dizaines de kilomètres) avec un débit important. Ainsi, un réseau métropolitain permet à deux machines distantes de communiquer comme si elles faisaient partie d'un même réseau local.

Un MAN est formé d'équipements réseau interconnectés par des liens hauts débits (en général en fibre optique).

Réseaux étendus (WAN)

Un réseau étendu (**WAN**, *Wide Area Network*) interconnecte plusieurs réseaux locaux à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des équipements réseau appelés **routeurs**, qui permettent de déterminer le trajet le plus approprié pour atteindre une machine du réseau.

Réseaux locaux virtuels (VLAN)

Un **VLAN** (*Virtual Local Area Network* ou *Virtual LAN*, en français *Réseau local virtuel*) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLAN), il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

□ Typologie de VLAN

Plusieurs types de VLAN¹ sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- Un **VLAN de niveau 1** (aussi appelé **VLAN par port** ou *Port-Based VLAN*) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur.
- Un **VLAN de niveau 2** (également appelé **VLAN MAC**, *VLAN par adresse IEEE* ou *MAC Address-Based VLAN*) définit un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le

1. Les VLAN sont définis par les standards IEEE 802.1D, 802.1p, 802.1Q et 802.10 : <http://www.ieee802.org/1>.

VLAN par port car le réseau est indépendant de la localisation de la station.

- Un **VLAN de niveau 3** : on distingue plusieurs types de VLAN de niveau 3 :
 - Le **VLAN par sous-réseau** (*Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
 - Le **VLAN par protocole** (*Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk...), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

□ Les avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- Plus de **souplesse pour l'administration et les modifications** du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en **sécurité** car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- **Réduction de la diffusion du trafic** sur le réseau.